Frédéric Dupuis

dupuis@fi.muni.cz • www.fi.muni.cz/~dupontd/

Personal information

- Birth: 29.08.1983 in Sept-Îles, Québec
- Citizenship: Canada
- Languages spoken: French (native), English (fluent), German (intermediate)

Education

Université de Montréal — **Montréal, Québec**
Ph.D. in Computer Science — *Sept 2005–Dec 2009*
Thesis title: *The decoupling approach to quantum information theory*
Advisors: Gilles Brassard and Patrick Hayden (McGill University)

University of Toronto — **Toronto, Ontario**
B.A.Sc, Engineering Science, Electrical Engineering option — *Sept 2001–May 2005*
Fourth-year thesis title: *Optimizing the key generation rate in decoy state quantum cryptography*
Advisor: Hoi-Kwong Lo

Academic Employment

Masaryk University — **Brno, Czech Republic**
Assistant Professor, Faculty of Informatics — *January 2017–*

Masaryk University — **Brno, Czech Republic**
Scientific Researcher, Faculty of Informatics — *September 2014–December 2016*
(This is an entry-level permanent position.)

Aarhus University — **Aarhus, Denmark**
Postdoctoral Researcher, Department of Computer Science — *January 2013–August 2014*
Group leader: Ivan Damgård

ETH Zürich — **Zürich, Switzerland**
Postdoctoral Researcher, Institute for Theoretical Physics — *January 2010–December 2012*
Group leaders: Renato Renner and Matthias Christandl

University of Toronto — **Toronto, Ontario**
Research Assistant, Electrical Engineering department — *May 2005–August 2005*
Supervisor: Wei Yu

University of Toronto — **Toronto, Ontario**
Research Assistant, Electrical Engineering department — *May 2004–August 2004*
Supervisor: Wei Yu

University of Toronto — **Toronto, Ontario**
Research Assistant, Electrical Engineering department — *May 2003–August 2003*
Supervisor: Wei Yu

Peer-reviewed journal articles

[1] Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl. "Catalytic decoupling of quantum information". In: *Phys. Rev. Lett.* 118 (Feb. 2017), p. 080503. DOI: 10.1103/PhysRevLett.118.080503. arXiv: 1605.00514.

[2] Frédéric Dupuis and Mark M. Wilde. "Swiveled Rényi entropies". In: *Quantum Information Processing* (2016), pp. 1–37. DOI: 10.1007/s11128-015-1211-x. arXiv: 1506.00981.

[3] Joseph M. Renes, David Sutter, Frédéric Dupuis, and Renato Renner. "Efficient quantum polar codes requiring no preshared entanglement". In: *IEEE Transactions on Information Theory* 61.11 (Nov. 2015), pp. 6395–6414. DOI: 10.1109/TIT.2015.2468084. arXiv: 1307.1136.

[4] Philippe Faist, Frédéric Dupuis, Jonathan Oppenheim, and Renato Renner. "The minimal work cost of information processing". In: *Nature Communications* 7669 (July 2015). DOI: 10.1038/ncomms8669. arXiv: 1211.1037.

[5] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. "Entanglement sampling and applications". In: *IEEE Transactions on Information Theory* 61.2 (Feb. 2015), pp. 1093–1112. DOI: 10.1109/TIT.2014.2371464. arXiv: 1305.1316.

[6] Frédéric Dupuis. "Chain rules for quantum Rényi entropies". In: *Journal of Mathematical Physics* 56.2, 022203 (2015). DOI: 10.1063/1.4907981. arXiv: 1410.5455.

[7] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. "One-shot decoupling". In: *Communications in Mathematical Physics* 328.1 (2014), pp. 251–284. DOI: 10.1007/s00220-014-1990-4. arXiv: 1012.6044.

[8] Frédéric Dupuis, Oleg Szehr, and Marco Tomamichel. "A decoupling approach to classical data transmission over quantum channels". In: *IEEE Transactions on Information Theory* 60.3 (Mar. 2014), pp. 1562–1572. DOI: 10.1109/TIT.2013.2295330. arXiv: 1207.0067.

[9] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. "On quantum Rényi entropies: a new generalization and some properties". In: *Journal of Mathematical Physics* 54.12, 122203 (2013). DOI: 10.1063/1.4838856. arXiv: 1306.3142 [quant-ph].

[10] Frédéric Dupuis, Jan Florjanczyk, Patrick Hayden, and Debbie Leung. "The locking-decoding frontier for generic dynamics". In: *Proceedings of the Royal Society A* 469.2159 (2013). DOI: 10.1098/rspa.2013.0289. arXiv: 1011.1612.

[11] Alexander Vitanov, Frédéric Dupuis, Marco Tomamichel, and Renato Renner. "Chain rules for smooth min- and max-entropies". In: *IEEE Transactions on Information Theory* 59.5 (2013), pp. 2603–2612. DOI: 10.1109/TIT.2013.2238656. arXiv: 1205.5231.

[12] Oleg Szehr, Frédéric Dupuis, Marco Tomamichel, and Renato Renner. "Decoupling with unitary approximate two-designs". In: *New Journal of Physics* 15.5 (2013), p. 053022. DOI: 10.1088/1367-2630/15/5/053022. arXiv: 1109.4348.

[13] Joseph M. Renes, Frédéric Dupuis, and Renato Renner. "Efficient Polar Coding of Quantum Information". In: *Physical Review Letters* 109 (5 Aug. 2012), p. 050504. DOI: 10.1103/PhysRevLett.109.050504. arXiv: 1109.3195.

[14] Simon Pierre Desrosiers and Frédéric Dupuis. "Quantum entropic security and approximate quantum encryption". In: *IEEE Transactions on Information Theory* 56.7 (July 2010), pp. 3455–3464. DOI: 10.1109/TIT.2010.2048488. arXiv: 0707.0691.

[15] Frédéric Dupuis, Patrick Hayden, and Ke Li. "A father protocol for quantum broadcast channels". In: *IEEE Transactions on Information Theory* 56.6 (June 2010), pp. 2946–2956. DOI: 10.1109/TIT.2010.2046217. arXiv: quant-ph/0612155.

[16] Frédéric Dupuis, Nicolas Gisin, Avinatan Hassidim, André Allan Méthot, and Haran Pilpel. "No nonlocal box is universal". In: *Journal of Mathematical Physics* 48.8, 082107 (2007), p. 082107. DOI: 10.1063/1.2767538. arXiv: quant-ph/0701142.

[17] Xiongfeng Ma, Fred Chi-Hang Fung, Frédéric Dupuis, Kai Chen, Kiyoshi Tamaki, and Hoi-Kwong Lo. "Decoy-state quantum key distribution with two-way classical postprocessing". In: *Physical Review A* 74 (3 Sept. 2006), p. 032330. DOI: 10.1103/PhysRevA.74.032330. arXiv: quant-ph/0604094.

Peer-reviewed conference publications

[1] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne, and Louis Salvail. "Adaptive versus non-adaptive strategies in the quantum setting with applications". In: *Proceedings of CRYPTO 2016*. 2016, pp. 33–59. DOI: 10.1007/978-3-662-53015-3_2. arXiv: 1607.08168.

[2] Ivan Damgård, Frédéric Dupuis, and Jesper Buus Nielsen. "On the orthogonal vector problem and the feasibility of unconditionally secure leakage-resilient computation". In: *Proceedings of ICITS 2015 (International Conference on Information-Theoretic Security)*. Full version available at http://eprint.iacr.org/2014/282. 2015, pp. 87–104. DOI: 10.1007/978-3-319-17470-9_6.

[3] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. "Achieving the limits of the noisy-storage model using entanglement sampling". In: *Proceedings of CRYPTO 2013*. 2013, pp. 326–343. DOI: 10.1007/978-3-642-40084-1_19. *Conference version of: "Entanglement sampling and applications" in the journal papers section*.

[4] David Sutter, Joseph M. Renes, Frédéric Dupuis, and Renato Renner. "Efficient quantum channel coding scheme requiring no preshared entanglement". In: *Proceedings of the 2013 IEEE International Symposium on Information Theory*. July 2013, pp. 354–358. DOI: 10.1109/ISIT.2013.6620247. arXiv: 1307.1136.

[5] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. "Actively Secure Two-Party Evaluation of Any Quantum Operation". In: *Proceedings of CRYPTO 2012*. Vol. 7417. Full version on IACR eprint archive: eprint.iacr.org/2012/304. 2012, pp. 794–811. DOI: 10.1007/978-3-642-32009-5_46.

[6] Frédéric Dupuis, Lea Krämer, Philippe Faist, Joseph M. Renes, and Renato Renner. "Generalized entropies". In: *Proceedings of the International Congress on Mathematical Physics*. World Scientific Publishing, Aug. 2012. arXiv: 1211.3141.

[7] David Sutter, Joseph M. Renes, Frédéric Dupuis, and Renato Renner. "Achieving the capacity of any DMC using only polar codes". In: *Information Theory Workshop (ITW), 2012 IEEE*. Sept. 2012, pp. 114–118. DOI: 10.1109/ITW.2012.6404638. arXiv: 1205.3756.

[8] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. "Secure two-party quantum evaluation of unitaries against specious adversaries". In: *Proceedings of CRYPTO 2012*. Springer, 2010, pp. 685–706. DOI: 10.1007/978-3-642-14623-7_37.

[9] Frédéric Dupuis. "The capacity of quantum channels with side information at the transmitter". In: *IEEE International Symposium on Information Theory*. June 2009, pp. 948–952. DOI: 10.1109/ISIT.2009.5205591. arXiv: 0805.3352.

[10] Frédéric Dupuis, Wei Yu, and Frans M. J. Willems. "Blahut-Arimoto algorithms for computing channel capacity and rate-distortion with side information". In: *IEEE International Symposium on Information Theory*. June 2004, p. 179. DOI: 10.1109/ISIT.2004.1365218.

Peer-reviewed conference talks without proceedings

[1] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. *Entropy accumulation in device-independent protocols*. QIP 2017 (Quantum Information Processing), Seattle, WA.

[2] Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl. *Catalytic decoupling of quantum information*. QIP 2017 (Quantum Information Processing), Seattle, WA.

[3] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne, and Louis Salvail. *Adaptive versus non-adaptive strategies in the quantum setting with applications*. QCrypt 2016 Conference, Washington DC. 2016. arXiv: 1607.08168.

[4] Ivan Damgård, Frédéric Dupuis, and Jesper Buus Nielsen. *A quantum protocol for the orthogonal vector problem and leakage-resilient computation*. QCrypt 2014 Conference, Paris, France, September 2014.

[5] Joseph M. Renes, David Sutter, Frédéric Dupuis, and Renato Renner. *Efficient secret key distillation over quantum channels*. QCrypt 2014 Conference, Paris, France, September 2014.

[6] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. *Entanglement sampling and applications*. QIP 2014 (Quantum Information Processing), Barcelona, Spain, February 2014.

[7] Frédéric Dupuis, Serge Fehr, Martin Müller-Lennert, Oleg Szehr, Marco Tomamichel, Mark Wilde, Andreas Winter, and Dong Yang. *A new quantum generalization of the Rényi divergence with applications to the strong converse in quantum channel coding*. QIP 2014 (Quantum Information Processing), Barcelona, Spain, February 2014.

[8] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. *Achieving the limits of the noisy-storage model using entanglement sampling*. QCrypt 2013 Conference, Waterloo, Ontario, August 2013.

[9] Joseph M. Renes, Frédéric Dupuis, and Renato Renner. *Quantum polar coding*. QIP 2012 (Quantum Information Processing), Montréal, Québec, December 2011.

[10] Frédéric Dupuis, Jan Florjanczyk, Patrick Hayden, and Debbie Leung. *The locking-decoding frontier for generic dynamics*. 6th Conference on Theory of Quantum Computation, Communication and Cryptography, Madrid, Spain, 24–26 May 2011.

[11] Simon Pierre Desrosiers and Frédéric Dupuis. *Quantum entropic security and approximate quantum encryption*. QIP 2008 (Quantum Information Processing), New Delhi, India, December 2007.

Preprints

[1] Frédéric Dupuis, Omar Fawzi, and Renato Renner. *Entropy accumulation*. 2016. arXiv: 1607.01796.

Invited Talks

Conferences and Workshops

- *Device-independent quantum cryptography via entropy accumulation*, Invited speaker, Central European Quantum Information Processing (CEQIP) Workshop, Smolenice, Slovakia, May 31 to June 3 2017.
- *Entropy accumulation*, Invited speaker, "Beyond i.i.d. in information theory" Workshop, Barcelona, Spain, July 18 to 22, 2016.
- *Entropy accumulation*, Invited speaker, Workshop on Quantum Cryptography and Quantum Computation, Aarhus University, Aarhus, Denmark, October 19 to 22, 2015.
- *Chain rules for quantum Rényi entropies*, Invited speaker, "Beyond i.i.d. in information theory" Workshop, Banff Internation Research Station, Banff, Canada, July 5 to 10, 2015.
- *Quantum error correction and polar codes*, Invited speaker, "New Frontiers of Quantum Information Theory" Workshop, Ascoli-Piceno, Italy, July 7 to 11, 2014.
- *Bounding the uncertainty of constrained adversaries*, Invited speaker, Central European Quantum Information Processing (CEQIP) Workshop, Znojmo, Czech Republic, June 5 to 8 2014.
- *On quantum Rényi entropies: a new definition and some properties*, "Beyond i.i.d. in information theory" Workshop, Centre for Quantum Technologies, National University of Singapore, Singapore, May 19 to 21 2014.
- *Bounding the uncertainty of constrained adversaries*, INTRIQ (Institut transdisciplinaire d'information quantique) spring meeting, Bromont, Québec, May 6 and 7 2014.
- *A new definition for the quantum conditional Rényi entropy*, "New Mathematical Directions for Quantum Information" Workshop, Isaac Newton Institute for Mathematical Sciences, Cambridge, England, Sept 2–6 2013.
- *Quantum two-party computation*. Workshop on Cryptography, Bellairs Research Institute, Barbados, March 3 to 7, 2013. (6-hour lecture miniseries.)
- *Classical coding via dequantizing*. Workshop "Beyond iid in information theory", Cambridge, England, January 8 to 11, 2013.
- *Efficient quantum polar coding*, Tsinghua-Aarhus CTIC Workshop on Quantum Information Science, Tsinghua University, Beijing, May 21, 2012.
- *Classical coding via decoupling*. Workshop "Quantum Information: Codes, Geometry and Random Structures" Centre de recherches mathématiques, Montréal, October 25, 2011.
- *Approximate quantum encryption and entropic security*. Invited speaker, Second QuantumWorks Annual General Meeting, Calgary, AB, September 26, 2007.
- *Introduction to quantum information theory*. Invited speaker, Workshop on One-Shot Quantum Information and Applications to Physics, Bellairs Research Institute, Barbados, March 12, 2007.
- *Practical Quantum Key Distribution with Decoy States*. Invited speaker, CIFAR Quantum Information Group Annual Meeting, Halifax, NS, June 2, 2005.

Seminars

- *A quantum protocol for the orthogonal vector problem and leakage-resilient computation*, Quantum Information group seminar, Universitat Autònoma de Barcelona (UAB), Barcelona, Spain, October 29, 2014.
- *Bounding the uncertainty of constrained adversaries*, Cryptology group seminar, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, Netherlands, July 4, 2014.
- *An introduction to "one-shot" quantum information theory*, Quantum information group seminar, Télécom Paris, Paris, France, April 29, 2014.
- *A tutorial on min- and max-entropies and their applications*, Quantum Information Seminar, Masaryk University, Brno, January 14, 2014.
- *Min-entropy sampling and cryptography in the bounded storage model*, Quantum Information Seminar, Leibniz-Universität Hannover, April 10, 2013.
- *Secure two-party quantum computation against specious adversaries*, Invited speaker, Colloquium of the Institute for Quantum Information, University of Waterloo, Waterloo, Ontario, March 21 2011.
- *The decoupling theorem*, Invited speaker, University of Bristol, October 2009.
- *The decoupling theorem*, Invited speaker, ETH Zürich, October 2009.
- *The decoupling theorem*, Invited speaker, National University of Singapore, September 2009.
- *Approximate quantum encryption and entropic security*. Invited speaker, Center for Quantum Information and Quantum Control, University of Toronto, October 26, 2007.

Pedagogical activities

- Teaching:
  - Seminar tutor, IV111 "Probability in Computer Science", Masaryk University, Spring 2017.
  - Seminar tutor, PB071 "Principles of low-level programming", Masaryk University, Spring 2017.
  - Seminar tutor, IB000 "Mathematical Foundations of Computer Science", Masaryk University, Fall 2016.
  - Seminar tutor, MA015 "Graph Algorithms", Masaryk University, Fall 2015 and 2016.
  - Seminar tutor, IB101 "Introduction to logic", Masaryk University, Spring 2015 and 2016.
  - Seminar tutor, IA170 "Randomness and Communication", Masaryk University, Fall 2015.
  - Seminar tutor, MA010 "Graph Theory", Masaryk University, Fall 2014.
  - Lecturer, "Quantum Information Processing" course at Aarhus University, First and second quarter of 2013–2014. I taught the second half of the course, the first half was taught by Ivan Damgård.
  - Teaching Assistant, Course IFT2105 (Theoretical Computer Science), Université de Montréal, Fall 2008. Professor: Alain Tapp

- Student supervision:
  - Luděk Matyska (Masters in Computer Science, Masaryk University, 2015–2016).
  - Martin Müller-Lennert (Masters in Mathematics, ETH Zürich, 2012–2013).
  - Emilio Onorati (Semester project and Masters in Physics, ETH Zürich, 2012–2013)
  - David Sutter (Masters in Electrical Engineering, ETH Zürich, 2012)
  - Richard Küng (Masters in Physics, ETH Zürich, 2012)
  - Alexander Vitanov (Masters in Physics, ETH Zürich, 2011)
  - Oleg Szehr (Semester project and Masters in Physics, ETH Zürich, 2010)
- Supervision of "Proseminar" projects, ETH Zürich. (This is a bachelors level class in which students must write a report and give an hour-long presentation on a particular topic in physics.)

Leadership, administration

- Program Committee member:
  - ICITS (International Conference on Information Theoretic Security) 2017, 29 Nov–2 Dec 2017, Hong Kong, China
  - CEQIP (Central European Quantum Information Processing) 2017, 31 May–3 June 2017, Smolenice, Slovakia
  - TQC (Theory of Quantum Computation, Communication and Cryptography) 2016, 27–29 Sept 2016, Berlin, Germany
  - QCrypt 2016, 12–16 Sept 2016, Washington DC, USA
  - ICITS (International Conference on Information Theoretic Security) 2016, 9–12 August 2016, Tacoma WA, USA
  - CEQIP (Central European Quantum Information Processing) 2016, 16–19 June 2016, Valtice, Czech Republic
  - CEQIP (Central European Quantum Information Processing) 2015, 18–21 June 2015, Telč, Czech Republic
  - TQC (Theory of Quantum Computation, Communication and Cryptography) 2015, 20–22 May 2015, Brussels, Belgium
  - ICITS (International Conference on Information Theoretic Security) 2015, 2–5 May 2015, Lugano, Switzerland
  - CEQIP (Central European Quantum Information Processing) 2014, 5–8 June 2014, Znojmo, Czech Republic
  - QCrypt 2014, 1–5 September, 2014, Paris, France
  - QCrypt 2013, 5–9 August, 2013, Waterloo, Canada
- Organizer (together with Sébastien Gambs) of the 2008 Canadian Quantum Information Students' Conference, Université de Montréal, June 16–20 2008

Prizes and awards

Scholarships

- NSERC (Natural Sciences and Engineering Research Council of Canada) Postdoctoral Fellowship, January 2010–December 2011 ($40000/year)

- NSERC Canada Graduate Scholarship–PhD Level, September 2006–September 2009 ($35000/year)
- NSERC Canada Graduate Scholarship–Masters level, September 2005–September 2006 ($17500)
- Marc-Bourgie Foundation Scholarship ($10000), 2008–2009
- J.-Armand-Bombardier Scholarship ($10000), 2007–2008
- Université de Montréal Admission Scholarship ($10000)
- Stanford Graduate Fellowship ($32300/year, declined), 2005
- Princeton University First Year Fellowship ($30713/year, declined), 2005
- NSERC Undergraduate Research Scholarship, Summer 2003.

Prizes

- Bronze Medal, 2001 International Physics Olympiad, Antalya, Turkey
- Honorable Mention, 2000 International Physics Olympiad, Leicester, UK
- First place in Canada, 2001 Canadian Association of Physicists Prize Exam
- Sixth place in Canada, 2000 Canadian Association of Physicists Prize Exam